712 Form

- Hardcopy – on file with MORS office

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
14 JUN 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
SUN-TZU: Proposal for an agent based battle staff planning tool foranalysis of situation awareness data anomalies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Research LaboratoryAberdeen Proving Ground, MD 21005**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM201946, Military Operations Research Society Symposium (73rd) Held in West Point, NY on 21-23 June 2005., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**34**	

SUN-TZU: Proposal for an agent based battle staff planning tool for analysis of situation awareness data anomalies

John Brand
Devin Burns
Ann Brodeen
Richard Kaste

US Army Research Laboratory
Aberdeen Proving Ground, MD 21005

Military Operations Research Society Symposium
June 2005
US Military Academy
West Point, NY

What is it?

- Sun-Tzu is a concept for an agent based situational awareness (SA) data base tool intended to find and highlight inconsistencies in the battle SA picture

- The goal is to find inconsistencies that might cue the existence of a deception story

- It is bottom-up, not top-down

- Sources of inconsistency other than deception might be tactically *much more valuable*:
  - incomplete detection—not sensing things that are there
  - mistaken detection or interpretation—wrong identification of sensed element
  - false detection—seeing what isn't there
  - mistaken interpretation—wrong picture of reality

Assumptions

- There is a lot of information available—too sparse and you are doomed anyway (Imperial Japan after 1941)
- The information is reasonably correct—too wrong and you are doomed anyway (Nazis after ~1940)
- Basic premise for countering—or implementing—deception with templates is that no deception story can be complete if examined closely enough
- Enemy deceptions *must* be included in set of templates
- Deception may be local or global—due to small unit commander initiative or centrally planned and executed—these will differ in techniques, resources
- Watch out for too good to be true
- This is not RAID—more on that later

Applications

- This analysis cues incongruities or anomalies in the Situation Awareness data base—

- One kind of incongruity or anomaly may underlie an enemy deception effort

- Others may be due to
  - mis-identifications,
  - non-detections,
  - false detections,
  - mis-interpretations

- At the *tactical* level these are far more likely, and may be *far more valuable than warning of possible deception per se*

Basic thesis

"The possibility of detecting deception… is inherent in the effort to deceive. Every deception operation necessarily leaves at least two clues:

incongruities about what is hidden; and

incongruities about what is displayed in (its) stead.

The analyst requires only the appropriate sensors and mindset (cognitive hypotheses) to detect and understand the meaning of these clues.

*(Whaley-Busby p. 191)."**

*From tutorial, Integrating Methods and Tools to Counter Denial and Deception, Ed Waltz, International Conference on Intelligence Analysis, 2 May 2005, courtesy Frank Stech, MITRE, used with permission.

>>The trick is how to find the clues.

How to do it?

• Basic tool is the template

• Evidence from the study of decision making indicates that, in situations with incomplete data and under time pressures, a high proportion (perhaps 96%*) of decisions are based on recognizing and applying patterns

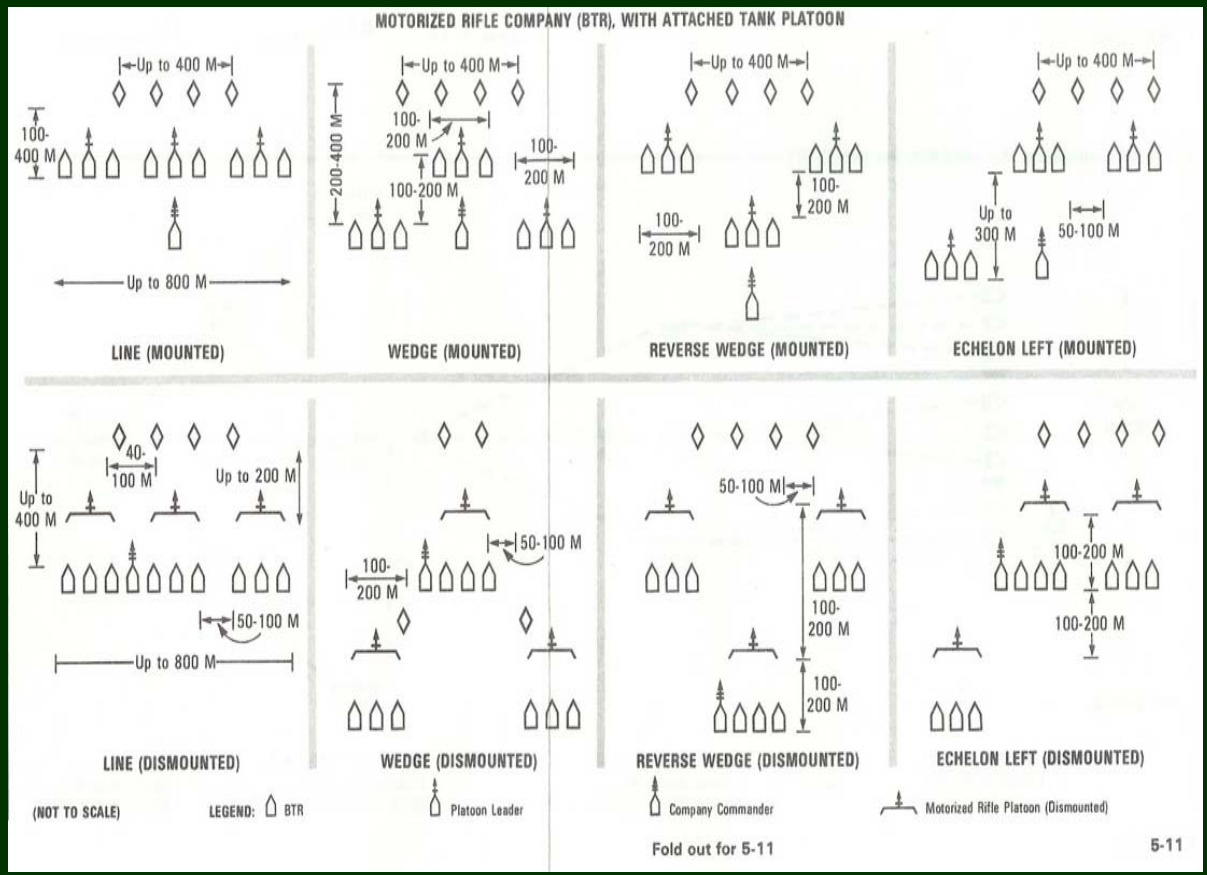
- Learned patterns are used to diagnose or recognize situations
- Learned patterns are used to implement solutions
- These patterns are doctrine, tactics, and at the lowest level, SOP and battle drill
- Some leaders will ignore or discard learned patterns and either blunder or innovate—the dummy or genius factor

* from Gary Klein, *Sources of Power*, The MIT Press, 1998, referenced at http://www.cs.mu.oz.au/~ejn/pubs/NorlingHeinze-CogSci00.pdf

What is a template?

- A template is a pattern of activity or things
- It can be compared to the elements of the situational awareness picture at all levels
- A template can be derived from enemy doctrine either published or deduced
- It can be applied piecewise to each datum in the SA picture at that level
- The degree of “fit” of the template to the data can be estimated several ways
- Template evaluation must provide a warning in the case of “too much” as well as “too little”

Example of a template starting point



From FM 100-2-1, The Soviet Army, Operations and Tactics, 16 July 1984. Although the Soviet Union is no more, a lot of people were trained in this way of waging war. In any case, the material is illustrative if not definitive.

Really really elementary example of use of a template

Consider a sensing of a vehicle identified as an armored vehicle.

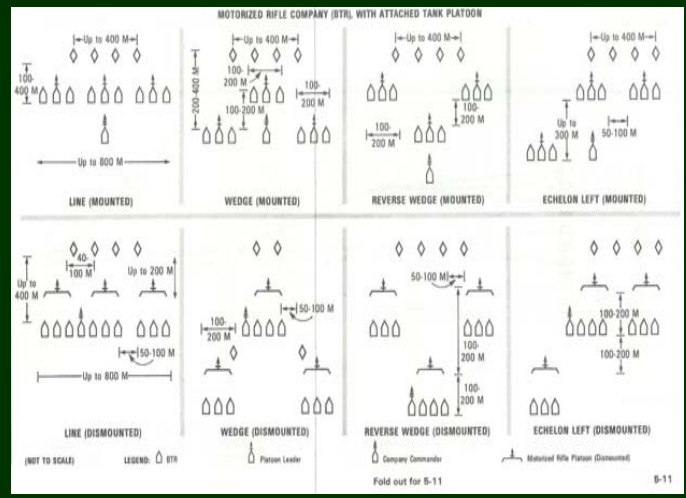
The sensing is accompanied by a constellation of other sensings. The sensing datum under consideration is examined to see if the other sensings correspond to the old-style Soviet geometric formations: is there another armored vehicle within 100 meters? 400 meters? Is it a tank? An APC or IFV? MTLB? Etc., etc.

If so, is there a command vehicle within 500 meters? A logistic vehicle within 1000 meters? Are the terrain and met conditions favorable for detection if the required vehicles were indeed there, if not sensed?

Is the same sensed set of vehicles present in sensings a day earlier? Two days? Three?

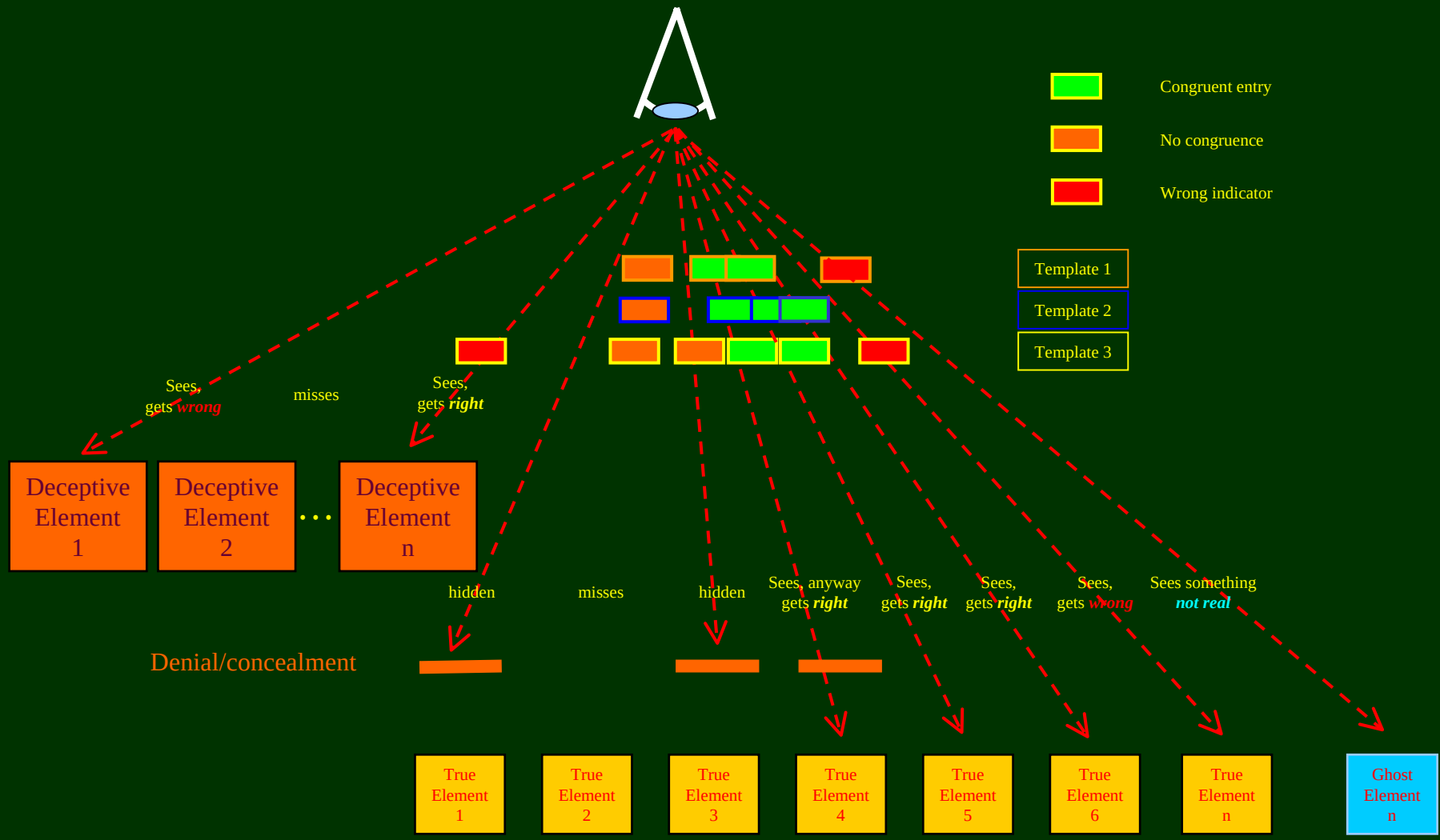
Does the sensing permit recognition of tracks? If so, are there any?

Does the ELINT data base include sensings of the proper type, say R123 radios? And so on.

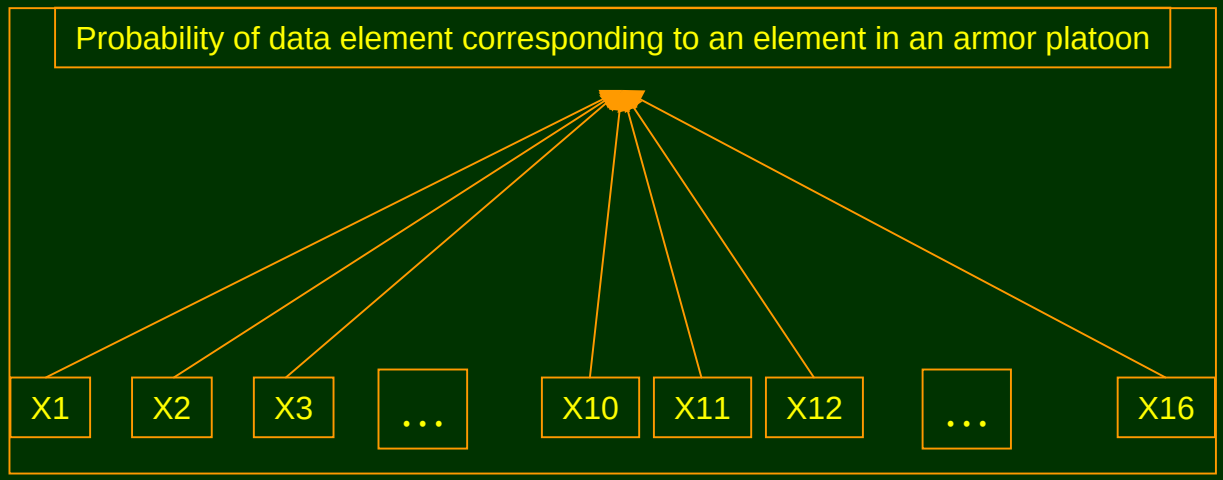


(from p. 5-11, FM 100-2-1, *The Soviet Army, Operations and Tactics*, 16 July 1984)

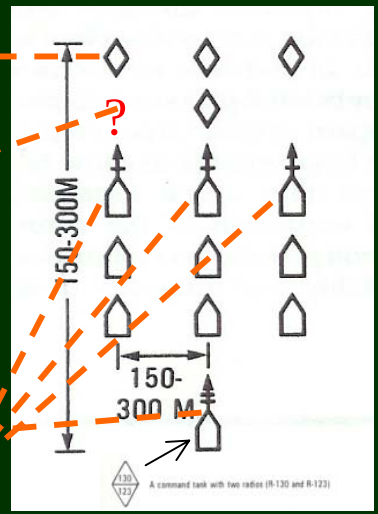
Templating


Congruent entry
No congruence
Wrong indicator
Template 1
Template 2
Template 3
Sees, gets wrong
misses
Sees, gets right
Deceptive Element 1
Deceptive Element 2
Deceptive Element n
hidden
misses
hidden
Sees, anyway gets right
Sees, gets right
Sees, gets right
Sees, gets wrong
Sees something not real
Denial/concealment
True Element 1
True Element 2
True Element 3
True Element 4
True Element 5
True Element 6
True Element n
Ghost Element n

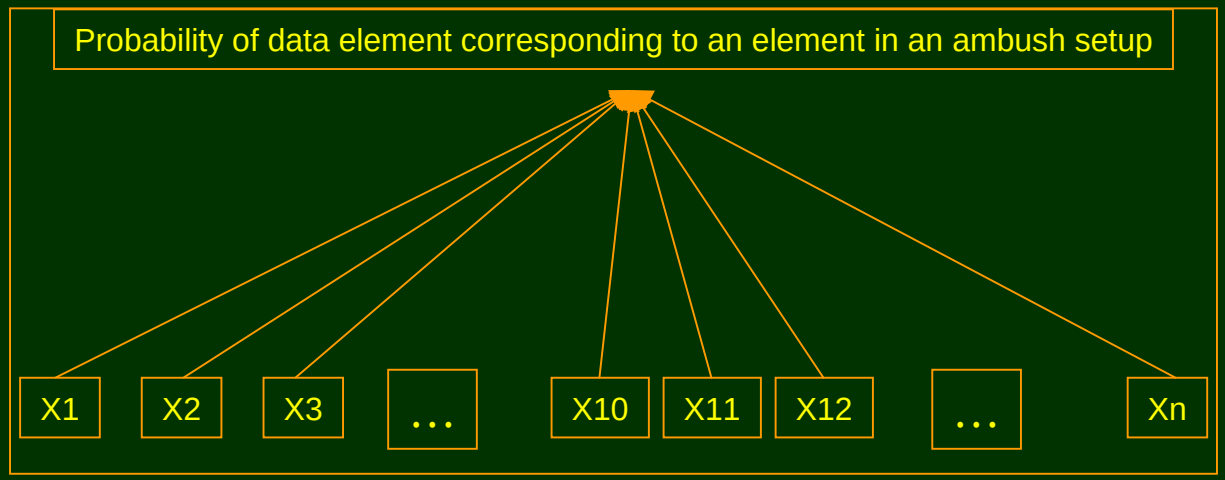
Simple low level tactical template



Datum X1: Visual signature tank 1--data element being parsed
Evidence datum X2: Visual signature tank 2
Evidence datum X3: Visual signature tank 3
Evidence datum X4: Visual signature tank 4
Evidence datum X5: Acoustic signature—idling tank engine sound
Evidence datum X6: Acoustic signature—moving tank
Evidence datum X7: Chemical signature—exhaust
Evidence datum X8: Thermal hot spot
Evidence datum X9: Radar return—conventional centimetric wavelength
Evidence datum X10: Millimeter wave radar
Evidence datum X11: Lidar signature
Evidence datum X12: Tracks on ground
Evidence datum X13: Communications signature
Evidence datum X14: Presence of controlling headquarters element
Evidence datum X15: Presence of accompanying units such as other tank or mechanized infantry platoons
Evidence datum X16: Terrain factors—is it suitable for vehicles? Tracked vehicles? Wheeled?



Simple low level deception template

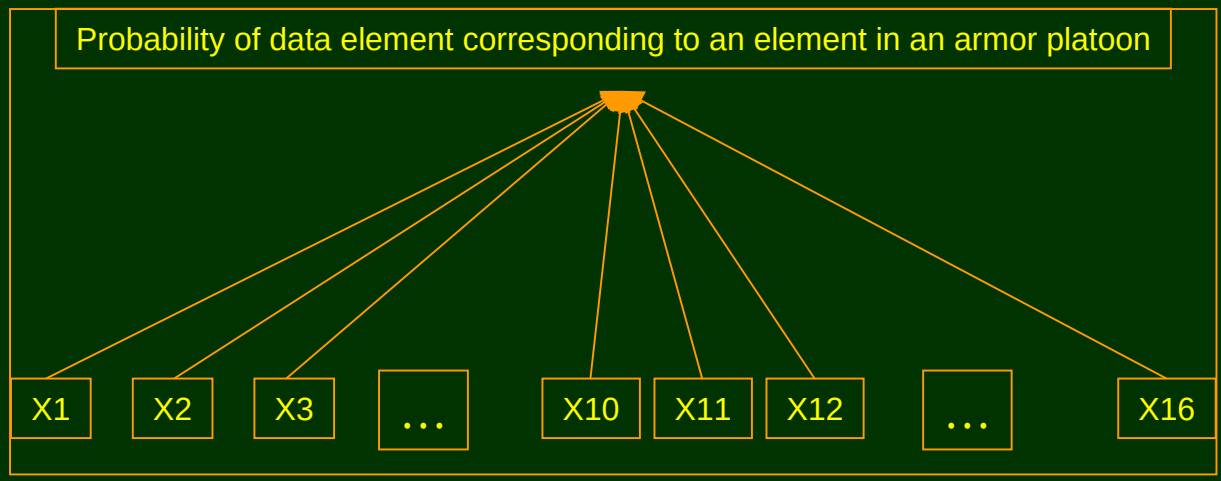


Visual signature tank 1—data element being parsed
Visual signature tank 2
Visual signature tank 3
Visual signature tank 4
Acoustic signature—idling
…..etc.
Tracks on ground
Communications
Presence of cmd. Element
Presence of accompanying units
Terrain factors—US access?
Enemy element in overwatch position?
Enemy artillery in range?
Commanding ground nearby?
Increasing terrain restriction?
Easy enemy retreat path?
Disturbed earth along path?
…….etc.

How to estimate congruence or divergence: metrics

- Problem is how to reduce these elements to some numerical value or metric
- Several possibilities
  - Add up the yeses/noes
  - Weight the elements and add, normalize, etc.: (Grey System Theory or normal ORSA stuff, take your pick)
  - Phase space vector manipulation
  - Bayesian Belief Network (BBN)

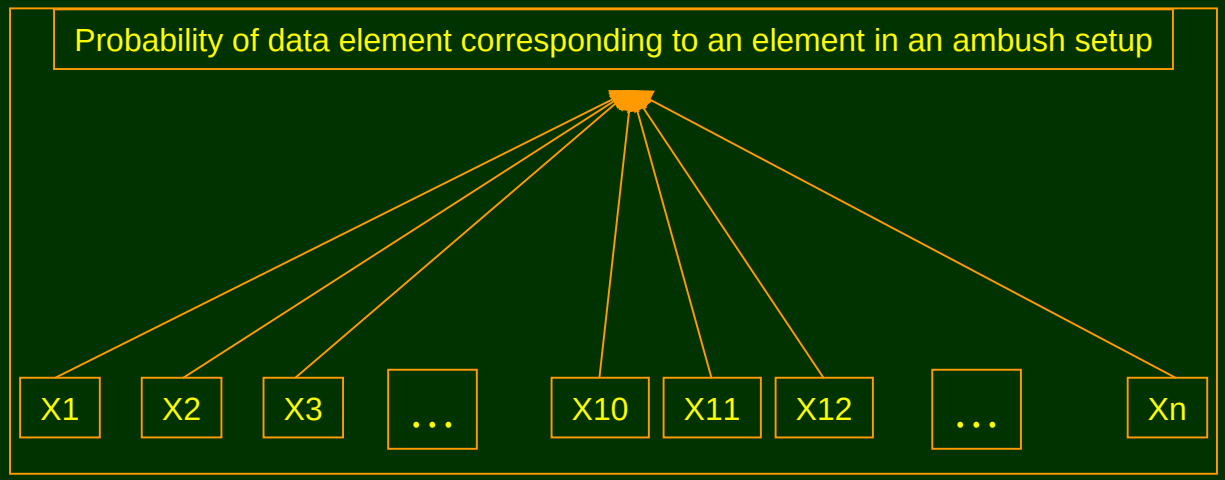
Simple pseudo-binary approach



Visual signature tank 1	data element being parsed	+1
Visual signature tank 2	not detected	0
Visual signature tank 3	detected 80 meters away	+1
Visual signature tank 4	not detected	0
Acoustic—idling	detected by array	+1
Acoustic—moving	not sensed	0
Chemical signature—exhaust	not sensed, no means to do so	0
Thermal	checked, not present	-1
Radar—conv. cm wavelength	not checked	0
Millimeter wave radar	not checked	0
Lidar	not checked	0
Tracks on ground	UAV checked, not found, ground suitable	-1
Communications	no ELINT	0
Presence of cmd. Element	not sensed, open ground	-1
Presence of accompanying units	not sensed, open ground	-1
Terrain factors—is it suitable?	No	-1
Total		-2/16: *probably not*

Just add up the yesses (+1s) and contradictions or noes (-1s or 0s), normalize to number of elements (16 in this case)

Simple low level deception template



Visual signature tank 1	data element being parsed	+1
Visual signature tank 2	not detected	0
Visual signature tank 3	detected 80 meters away	+1
Visual signature tank 4	not detected	0
Acoustic signature—idling	yes, detected by array	+1
…..etc.		
Tracks on ground	UAV checked, tracks found, ground suitable	+1
Communications	recent xmissions at position	+1
Presence of cmd. Element	not sensed, open ground	-1
Presence of accompanying units	not sensed, open ground	-1
Terrain factors—US access?	yes	+1
Enemy element in overwatch position?	Not sensed, cover at positions	0
Enemy artillery in range?	Yes	+1
Commanding ground nearby?	Yes	+1
Increasing terrain restriction?	Yes	+1
Easy enemy retreat path?	Yes	+1
Disturbed earth along path?	Not sensed	0
…….etc.		

Linear deviation metric

- Consider the sum of the values resulting from correspondences of the elements of a template and the elements in a data base, weighted by their judged importance.
- Initially the value of correspondence of the *i*th element may be binary: 0 or 1.
- A refinement might be to include an estimate of the probability of the element in the data base being a true sensing, so that the values might range from 0 to 1, inclusive.
- Normalization allows comparison between templates, which might well have different numbers of potentially evidentiary data elements
- In this case the deviation metric might be

$$F(template\ TRUE) = Congruence = {}^{1}\!/_{N} \sum_{i} (weight)*(truth)_i$$

$$Deviation = 1 - Congruence$$

Phase space deviation metric

- The description of battle has been considered as a vector in an n-dimensional phase space.
- This leads to the possibility of a template being considered a vector in that phase space.
- There are several possible deviation vector measures.
- One is the dot-product of the phase space data elements and the template.
- In this case if the template fit the situational data each element of the template would be accompanied by a datum corresponding to it in the data base. In a first approximation the elements of the presumed detection either correspond to the template or they do not; that is, the confidence in the sensings or the trafficability data or accuracy of the acoustic signature in the situational awareness data base is presumed to be zero or unity.

$$Congruence = {}^{1}\!/_{N} \sum_{i} (weight\ of\ template\ element)_i (template\ element)_i * \frac{(corresponding\ database\ element)_i}{(\max value\ of\ corresponding\ database\ element)_i^{\,2}}$$

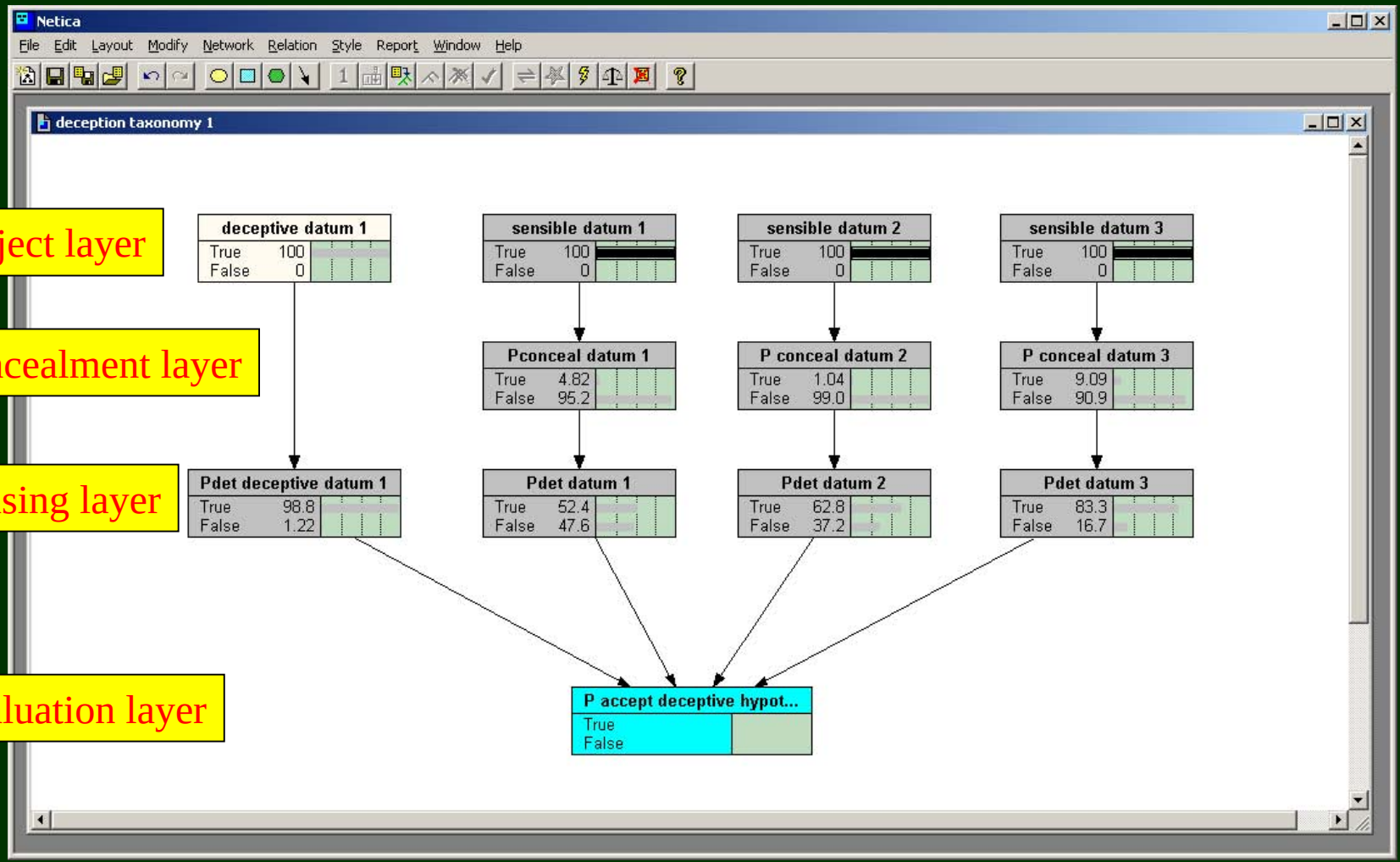
$$Deviation = 1 - Congruence$$

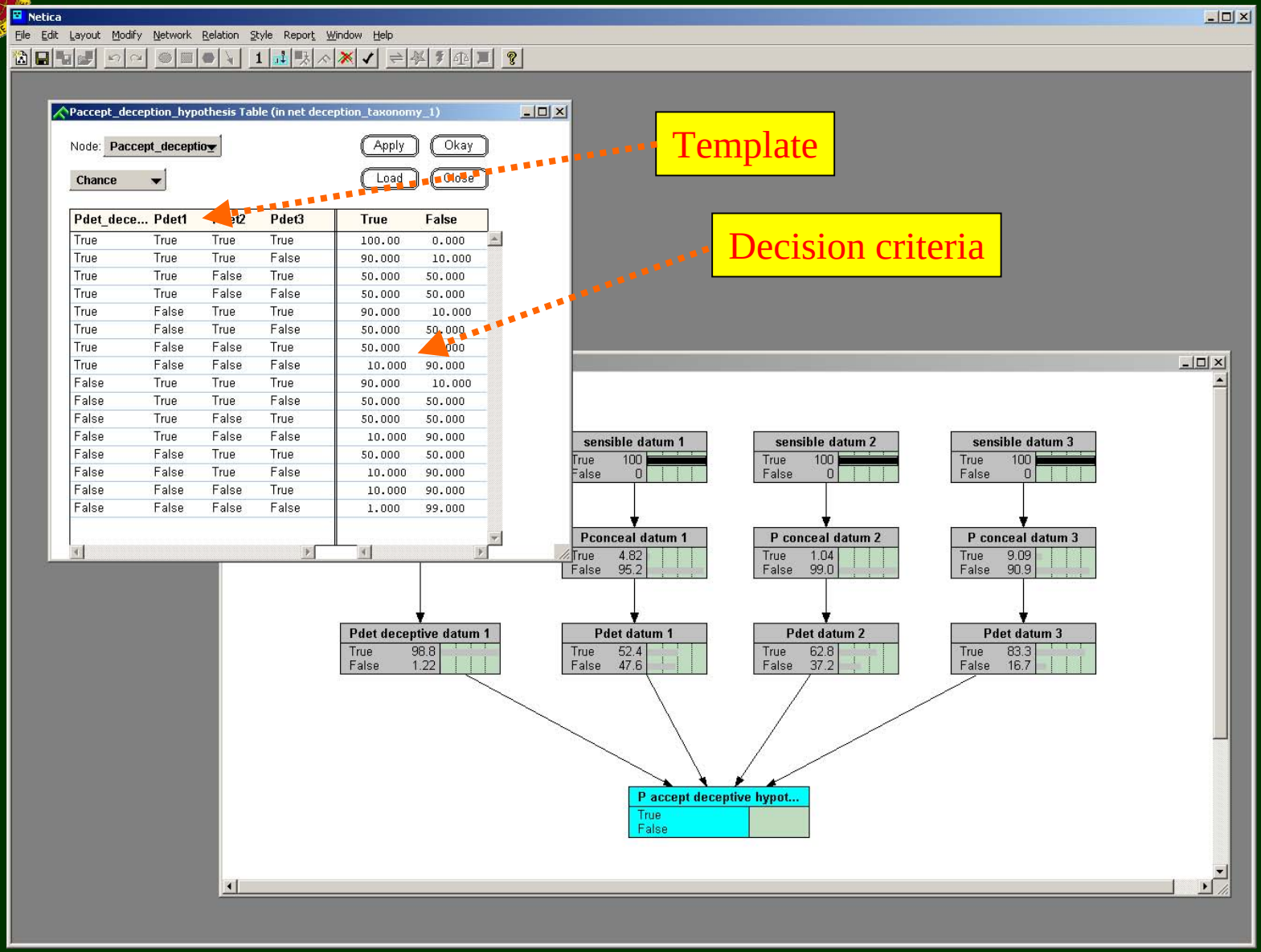
Bayesian Belief Network (BBN)

- Probability calculation of causes based on observed effects
- Cause → Target of interest, unknown event, etc.
- Effects → Trafficability Data, Acoustic Signatures, etc.
- Probabilities established based on prior information (templates)
- Bayes' Theorem for n basic events, A_1, A_2, ...A_n:

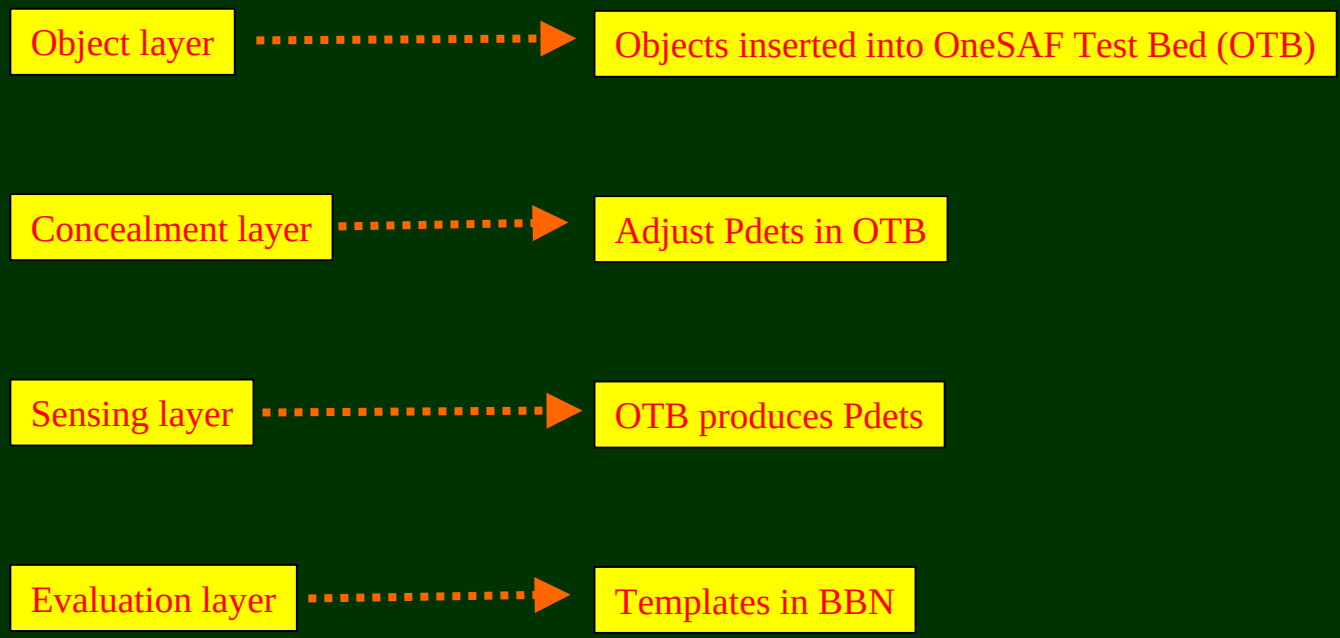
$$P(A_1 \mid B) = \frac{P(A_1)P(B \mid A_1)}{P(A_1)P(B \mid A_1) + P(A_2)P(B \mid A_2) + \cdots + P(A_n)P(B \mid A_n)}$$

Example BBN in Netica




Netica
File Edit Layout Modify Network Relation Style Report Window Help
Paccept_deception_hypothesis Table (in net deception_taxonomy_1)
Node: Paccept_deceptio
Apply
Okay
Load
Close
Chance
Pdet_dece... Pdet1 Pdet2 Pdet3 True False
True True True True 100.00 0.000
True True True False 90.000 10.000
True True False True 50.000 50.000
True True False False 50.000 50.000
True False True True 90.000 10.000
True False True False 50.000 50.000
True False False True 50.000 50.000
True False False False 10.000 90.000
False True True True 90.000 10.000
False True True False 50.000 50.000
False True False True 50.000 50.000
False True False False 10.000 90.000
False False True True 50.000 50.000
False False True False 10.000 90.000
False False False True 10.000 90.000
False False False False 1.000 99.000
Template
Decision criteria
sensible datum 1
True 100
False 0
sensible datum 2
True 100
False 0
sensible datum 3
True 100
False 0
Pconceal datum 1
True 4.82
False 95.2
P conceal datum 2
True 1.04
False 99.0
P conceal datum 3
True 9.09
False 90.9
Pdet deceptive datum 1
True 98.8
False 1.22
Pdet datum 1
True 52.4
False 47.6
Pdet datum 2
True 62.8
False 37.2
Pdet datum 3
True 83.3
False 16.7
P accept deceptive hypot...
True
False

Incongruity detection process



Interesting possibilities

- Deceptive activities and their templates are associated with a characteristic scale or coherence length in space and time
- An agent based approach may be able to access data appropriate to all these scales
- Sparseness of data in local SA data base introduces graininess and hence variation that may mask patterns at lower scales
- Access to multiple scales may compensate for this to some degree
- Insertion of deception or systematic error as an explicit layer may allow training the network by splitting of data set

Problems to solve

- Stech points out that you have to work on at least three levels—obvious, cross, double cross (paraphrase)
- Templates must accommodate this—hard to do, templates become very involved
- Templates of deception must be included—dependent on culture, enemy doctrine, military history
- Templates must change with time, circumstance—this can be accommodated by adding new templates
- Enemy deception doctrine is key

A note on RAID

The Defense Advanced Research Agency (DARPA) is presently developing the Real Time Adversarial Intelligence and Decision Making (RAID) tool.*

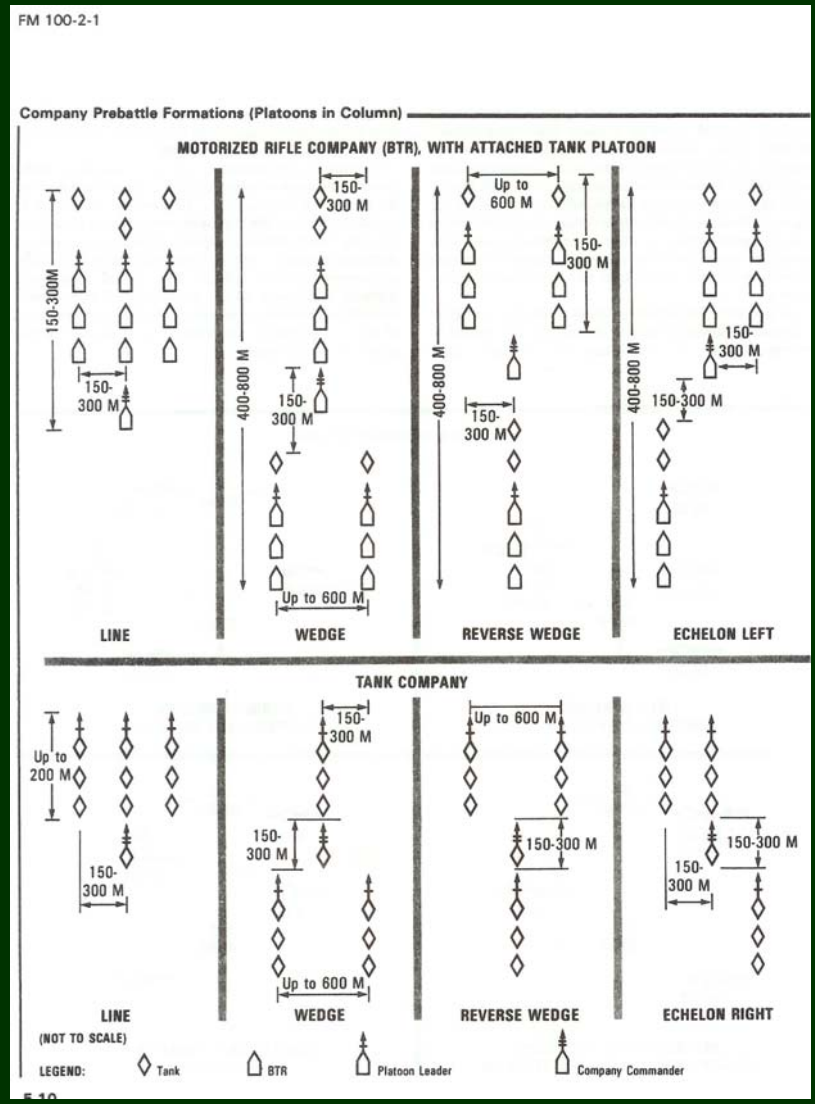
- RAID will take three years from contract award to bear fruit.
- The RAID deception module is defensive only.
- RAID is ambitious and hence high risk.
- The deception module will likely be dependent on the rest of the tool, especially the Adversarial Reasoning Model. If any of the whole does not work it risks usability of any component.
- RAID as envisaged in its initial phase will be a tactical level tool only.

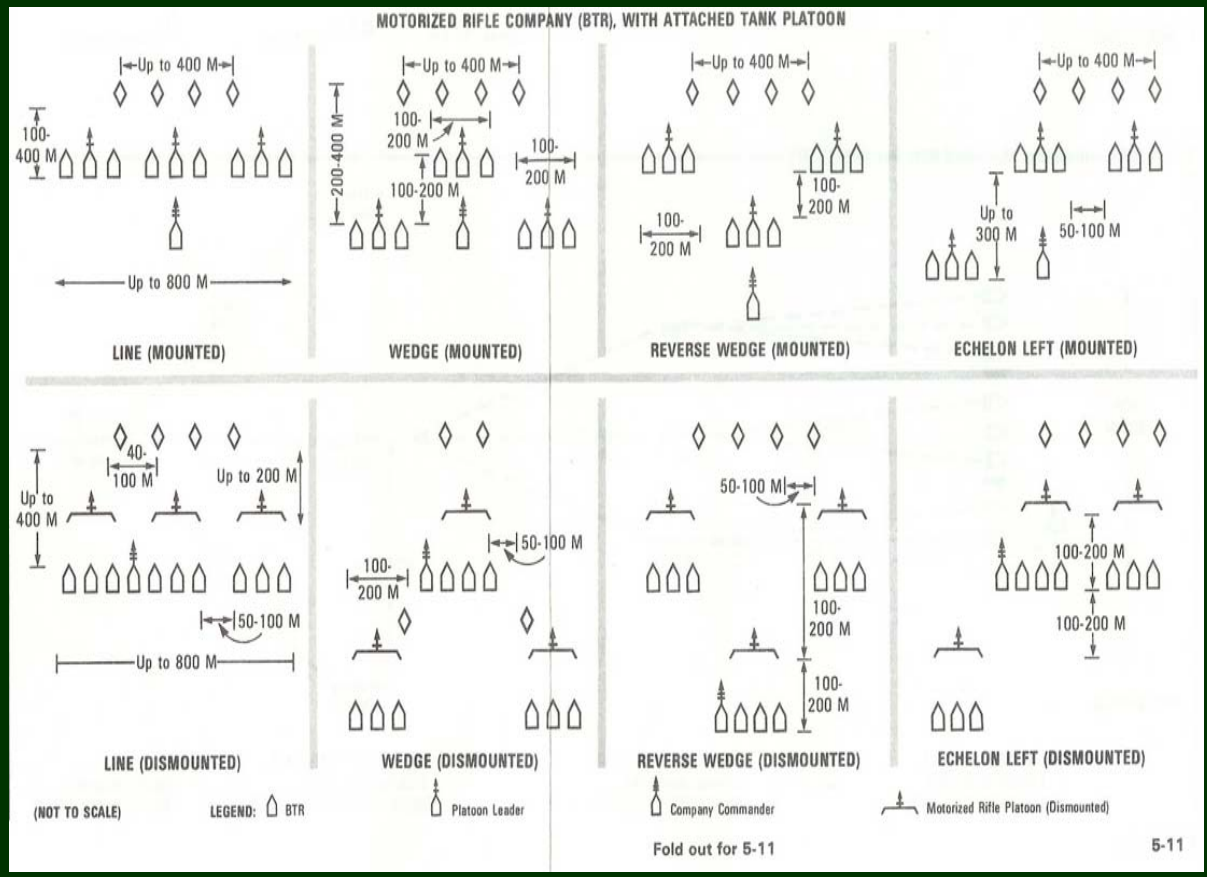
* See http://dtsn.darpa.mil/ixo/solicitations/raid/index.htm, accessed 3 January 2005.

Summary

- The opportunity exists to develop a data base tool that may have substantial benefits in lower level operations, including cuing of possible deception
- This tool will take a bottom-up approach to the analysis
- The next step is to:
  - Choose or devise a simplified surrogate data base,
  - Devise a set of templates,
  - Devise and test several metrics for determining fit of the metrics to the data,
  - Estimate the utility of measures of the fit to improve both the commander's and battle staff's interpretation of the situation.

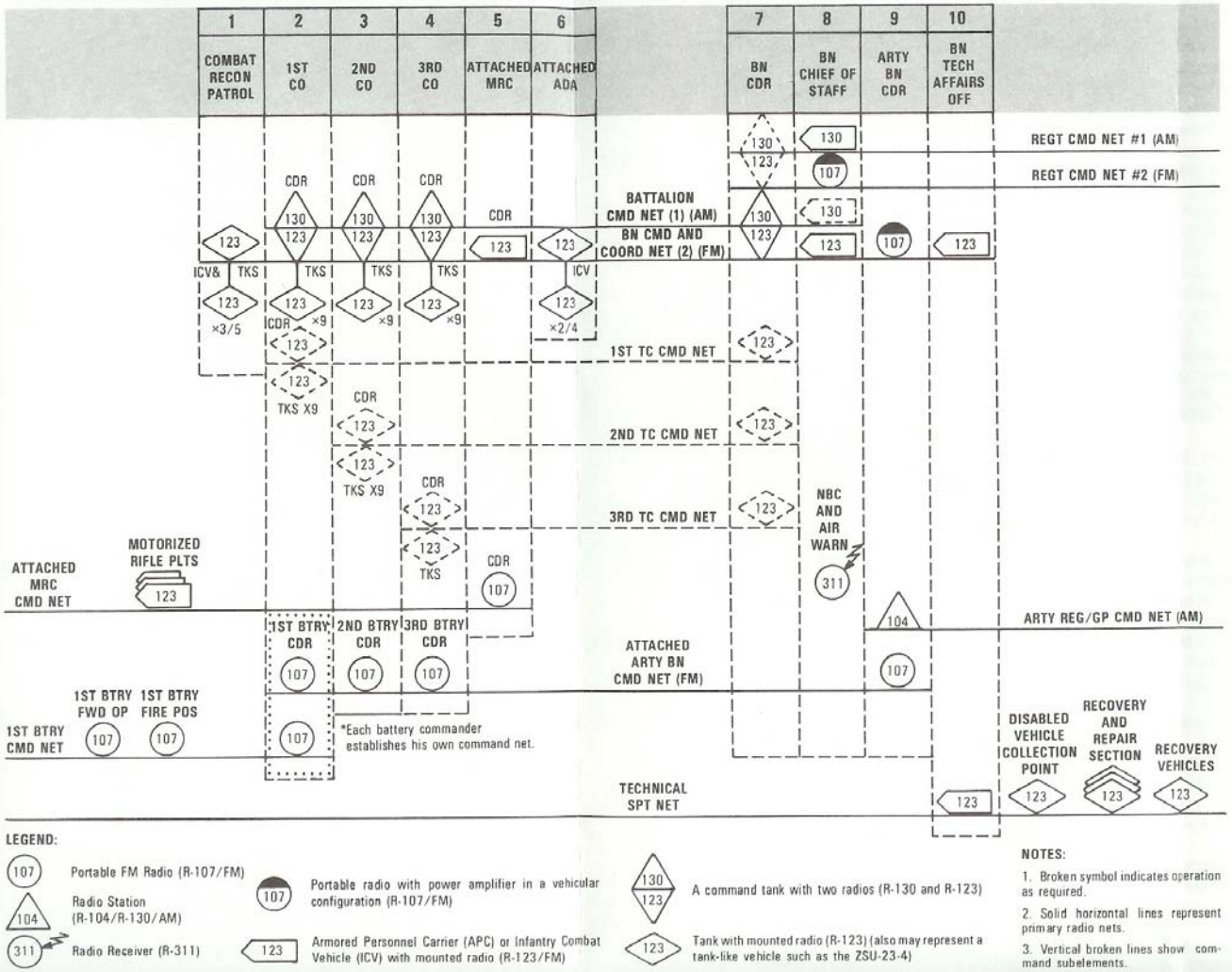
Backups

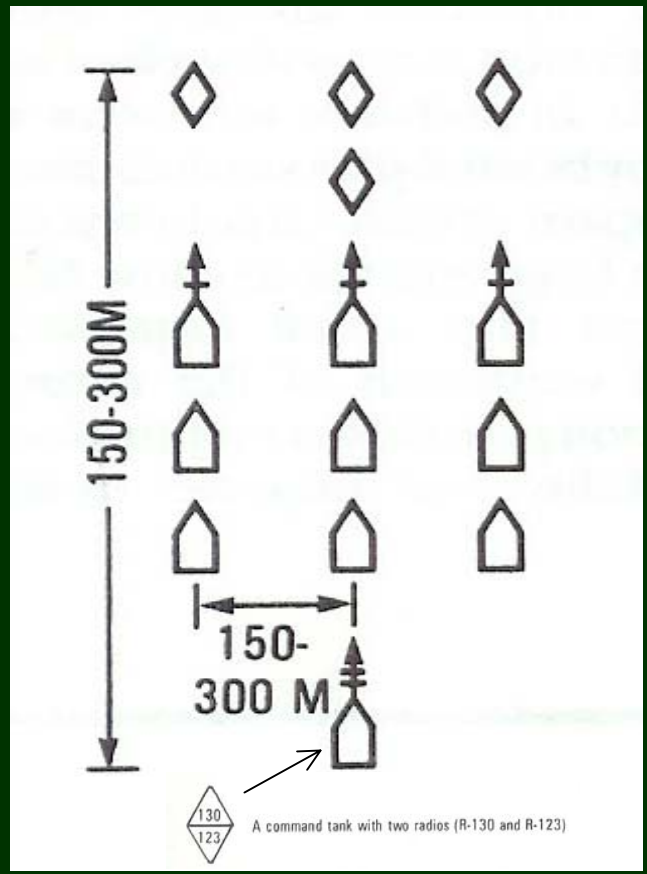

FM 100-2-1
Company Prebattle Formations (Platoons in Column)
MOTORIZED RIFLE COMPANY (BTR), WITH ATTACHED TANK PLATOON
150-300M
150-300 M
400-800 M
Up to 600 M
Up to 600 M
LINE
WEDGE
REVERSE WEDGE
ECHELON LEFT
TANK COMPANY
Up to 200 M
Up to 600 M
LINE
WEDGE
REVERSE WEDGE
ECHELON RIGHT
(NOT TO SCALE)
LEGEND:
Tank
BTR
Platoon Leader
Company Commander


MOTORIZED RIFLE COMPANY (BTR), WITH ATTACHED TANK PLATOON
Up to 400 M
100-400 M
Up to 800 M
LINE (MOUNTED)
200-400 M
100-200 M
WEDGE (MOUNTED)
REVERSE WEDGE (MOUNTED)
Up to 300 M
50-100 M
ECHELON LEFT (MOUNTED)
40-100 M
Up to 200 M
LINE (DISMOUNTED)
WEDGE (DISMOUNTED)
REVERSE WEDGE (DISMOUNTED)
ECHELON LEFT (DISMOUNTED)
(NOT TO SCALE)
LEGEND:
BTR
Platoon Leader
Company Commander
Motorized Rifle Platoon (Dismounted)
Fold out for 5-11
5-11

RADIO NETS, REINFORCED TANK BATTALION (VARIANT)

Shown here is a radio net diagram of a tank battalion to which an entire artillery battalion is attached for support. A tank battalion normally would be directly supported by an entire artillery battalion if it were fighting in the first echelon, or if it were operating separately from its parent regiment, as it might in a pursuit.




150-300M
150-
300 M
130
123
A command tank with two radios (R-130 and R-123)

Methods: Harris Inference from Ambiguities

Process	Description	Modes
Reconstructive Inference	•**Detect the presence of spurious signals (*sprignals*) that are indicators of D&D** • **Apply templates** predicted by conjectured pre-existing D&D hypotheses: •Strong evidence confirming hypothesis A (the simulation), •Weak contradictory evidence of hypothesis C (leakage from the adversary's dissimulation effort), •Missing evidence that should be present if hypothesis A were true.	Deduction
Incongruity Testing And Inference	• **Search for inconsistencies in the data (changes, anomalies, contradictions)** • **Synthesize (conjecture)** alternative explanations that attribute the incongruities to D&D (i.e. D&D explains the incongruity of evidence for more than one reality in simultaneous existence) • **Induce generalizations** (as appropriate, when tested and confirmed).	Deduction, then, Abduction, then, Induction

Integrating Methods and Tools to Counter Deception © Ed Waltz 2005 Page 29

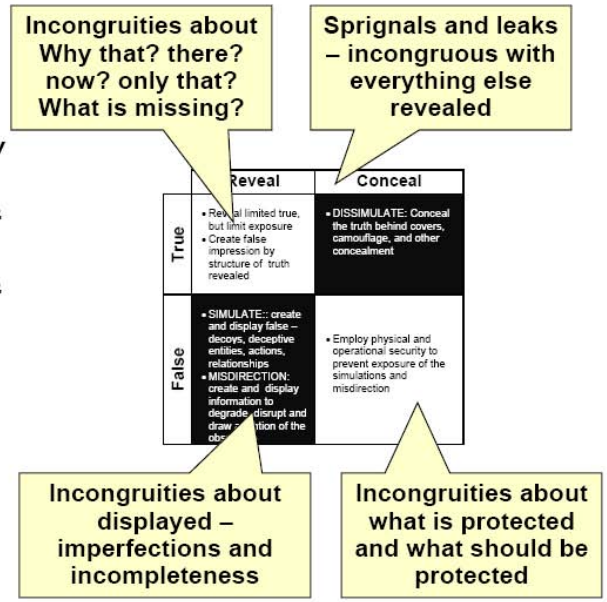
Courtesy Frank Stech, MITRE, from Mr. Waltz's tutorial, used with permission

Methods :Whaley-Busby Incongruities

"The possibility of detecting deception, is inherent in the effort to deceive. Every deception operation necessarily leaves at least two clues:

- *incongruities about what is hidden; and*
- *incongruities about what is displayed in it's stead.*

The analyst requires only the appropriate sensors and mind-set (cognitive hypotheses) to detect and understand the meaning of these clues." (Whaley-Busby p. 191).



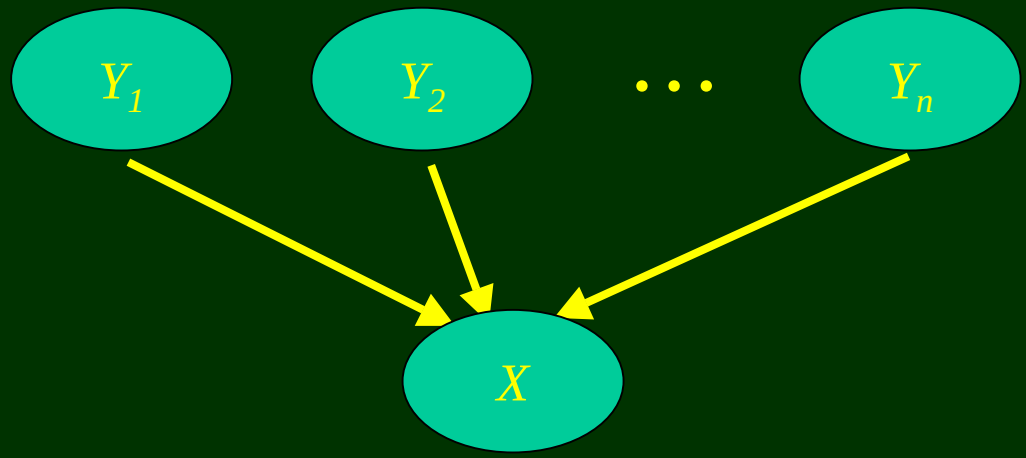
Courtesy Frank Stech, MITRE, from Mr. Waltz's tutorial, used with permission

Example

- 1% of a country's inhabitants are infected with a disease:
  - Let A_1 = infected population → $P(A_1) = 0.01$
  - Let A_2 = uninfected population → $P(A_2) = 0.99$
- An imperfect diagnostic test has been developed:
  - Let B = a test confirming infection → $P(B|A_1) = 0.97$ and $P(B|A_2) = 0.05$

- $$P(A1|B) = \frac{P(A_1)P(B \mid A_1)}{P(A_1)P(B \mid A_1) + P(A_2)P(B \mid A_2)}$$
- $$P(A1|B) = \frac{(0.01)(0.97)}{(0.01)(0.97) + (0.99)(0.05)}$$
- $$P(A1|B) = 0.16$$

Bayesian Belief Network (BBN)



$$P(x) = \Sigma P(x \mid y_1, y_2, \ldots y_n) P(y_1) P(y_2) \ldots P(y_n)$$

(Adapted from http://ai.stanford.edu/~koller/BNtut/sld061.htm, accessed 3 June 2005)